authorized to provide network resources, while being unable to retrieve and display information resources.

When client system 10 is periodically instructed to verify the authorization of server 60, client message generation module 58 creates an encrypted client message that is sent to the server via network infrastructure 52. In one embodiment, the encrypted client message includes a random number selected by client system 10. A detailed description of the components of the client message and the methods for creating the client message and generating random numbers is provided below in reference to Figure 4.

Server system 60 of Figure 3 is authorized to provide network resources to client system 10. Thus, server system 60 is capable of decrypting the client message using client message decryption module 62. Based on the information included in the client message, a client authorization module 64 determines the level of functionality that client system 10 is authorized to exhibit and determines the next time that the client system is to repeat the authorization process. The random number encoded in the client message and information specifying the client's authorized level of functionality and the next time that the client is to initiate reauthorization process are included in an encrypted service message created by service message generation module 66. It is noted that had server system 60 been not authorized to provide network resources to client system 10, it would have been incapable of decrypting the client message. Any random number included in the client message would have remained inaccessible by the unauthorized client, and any service message could not have included the random number.

Client system 10 receives the encrypted service message and decrypts it using service message decryption module 68. A message comparator module 70 compares the contents of the service message with the contents of the client message. In particular, in

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

embodiments employing random numbers, message comparator module 70 determines whether the service message contains the same random number as the client message. If so, client system 10 assumes that server system 60 is authorized to provide network resources, and system enabler module 56 permits the authorized network resources to be received and displayed or otherwise communicated to a user of the client system. If, however, message comparator module 70 determines that the service message does not contain the same random number as the client message, client system 10 assumes that server system 60 is not authorized, and system enabler module 56 disables some or all of the non-essential functions of the client system.

Figures 4 and 5 illustrate in greater detail the elements and functions of the client systems and authorized server systems according to one embodiment of the invention. Figure 4 depicts client system 10, which is illustrated as having three functional subsystems: system enablement subsystem 72, client message generation subsystem 74, and message comparison subsystem 76. Likewise, Figure 5 depicts server system 60 as having three functional subsystems: client message decryption subsystem 78, client authorization subsystem 80, and service message generation subsystems 82. The foregoing subsystems are presented to conveniently describe the structure and functions of client system 10 and server system 60 in the following discussion. In particular, the subsystems of client system 10 and server system 60 will be addressed below in the order that they are used in a typical process of verifying the authorization of the server system according to the invention.

Turning to Figure 4, client system 10 includes a security counter 84 and an expiration count 86 that together determine the moments at which the server verification procedures of the invention are initiated. Expiration count 86 has been set to specify when the server verification procedure is to begin. Security counter 84 is a timer or clock that

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

repeatedly increments the value of a security count until the security count reaches or exceeds the value of expiration count 86. Count comparator 88 monitors security counter 84 and, when the security count reaches or exceeds expiration count 86, the count comparator asserts an authorization interrupt. Security counter 84 and count comparator 88 constitute one example of a timing mechanism for specifying the times at which the client is to assert an authorization interrupt. In response to the authorization interrupt, a grace period timer 90 counts down an allotted grace period. If client system 10 fails to verify the authorization of server system 60 to provide network resources before the expiration of the allotted grace period, system enabler 91 will disable some or all of the non-essential functions of the client system.

The authorization interrupt asserted by count comparator 88 initiates activity in client message generation subsystem 74. In other circumstances, authorization interrupts can be created upon turning on client system 10 or at other times specified by software operating on the client system. To begin the process of verifying the authorization of server system 60, random number generator 92 generates a random number. In a preferred embodiment, random number generator 92 generates a unique signature based on asynchronous or external input conditions. For example, random number generator 92 can be a linear feedback shift register ("LFSR") seeded by asynchronous input according to techniques that will be understood by those skilled in the art. While numbers generated by an LFSR or by other conventional devices are technically pseudorandom, for purposes of this disclosure they will be designated as random. Random numbers generated by LFSRs or by other comparable systems provide the advantage of essentially eliminating the opportunity for other computers to generate random numbers in lockstep with client system 10.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111